Christopher L. Springer (SBN 291180)
KELLER ROHRBACK L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Tel: (805) 456-1496
cspringer@kellerrohrback.com

Cari Campen Laufenberg (*pro hac vice* forthcoming)
Gretchen Freeman Cappio (*pro hac vice* forthcoming)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel: (206) 623-1900
claufenberg@kellerrohrback.com
gcappio@kellerrohrback.com

Attorneys for Plaintiff Camie Picha

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

Camie Picha, individually and on behalf of others similarly situated,

Plaintiff,

v.

23andMe, Inc.,

Defendant

No.

COMPLAINT—CLASS ACTION

JURY DEMAND

TABLE OF CONTENTS

1. Plaintiff Camie Picha ("Plaintiff"), individually and for all others similarly situated, brings this action against Defendant 23andMe, Inc. ("23andMe" or "Defendant") on behalf of the victims of a targeted cyberattack on 23andMe that was announced on October 6, 2023 ("the Data Breach"). Plaintiff's and Class Members' most sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information")—including but not limited to name, sex, date of birth, genetic information, predicted relationships with genetic matches, ancestry reports, ancestors' birth locations and family names, family tree information, profile pictures, and geographic location—was compromised and exfiltrated in the data breach announced by 23andMe on October 6, 2023 (the "Data Breach").[1] Plaintiff brings this action against Defendant 23andMe for its failure to properly secure and safeguard the Private Information of herself and all those similarly situated, seeking monetary damages, restitution, and/or injunctive relief. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only 23andMe (as well as the cybercriminals who perpetrated the Data Breach) have knowledge of what information was compromised, Plaintiff reserves the right to supplement these allegations with additional facts and injuries as they are discovered.

[1] 23andMe, Inc., *Addressing Data Security Concerns,* 23andMe Blog (Dec. 5, 2023, 2:45 PM PST), https://blog.23andme.com/articles/addressing-data-security-concerns; *see also* Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023, 5:53 PM), https://www.wired.com/story/23andme-credential-stuffing-data-stolen/.

I. INTRODUCTION

2. 23andMe collects and maintains the genetic information of its customers—one of if not the most personal and highly sensitive forms of personally identifiable information and protected health information in existence. 23andMe profits from the highly sensitive Private Information that it collects and maintains, including through providing direct-to-consumer genetic testing services. 23andMe recognizes that it has an enormous responsibility to protect this highly sensitive Private Information, and it assures consumers through its Privacy and Data Protection statement that 23andMe "exceed[s] industry data protection standards and have achieved 3 different ISO certifications to demonstrate the strength of our security program."[2] Likewise, its Privacy and Data Protection statement acknowledges that its consumers "entrust us with important personal information," because of which, "since day one, protecting your privacy has been our number one priority," and 23andMe is "committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected." However, 23andMe completely failed to meet these promises and responsibilities to protect the Private Information of millions of its customers. Instead, 23andMe suffered a massive Data Breach in which the most highly sensitive Private Information of approximately 7 million of its consumers was compromised.

II. JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists, as Defendant is a citizen of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

4. This Court has personal jurisdiction over 23andMe because 23andMe is headquartered in California, within this District; 23andMe has its principal place of business in Santa Clara County, California, within this District; and 23andMe is authorized to and regularly

[2] 23andMe, Inc., *Addressing Data Security Concerns*, 23andMe Blog, https://blog.23andme.com/articles/addressing-data-security-concerns.

conducts business in the State of California, including by selling, marketing, and advertising its products and services to Class Members located in the State of California and within this District. 23andMe therefore has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

5. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) through (d) because 23andMe's principal place of business is located in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District.

III. DEFENDANT

6. Defendant 23andMe, Inc. is a business incorporated under the laws of the state of Delaware with its principal place of business in California, at 223 North Mathilda Avenue in Sunnyvale, California 94086. 23andMe is a genetic testing company that designs its products in California, and its marketing efforts emanate from California.

7. 23andMe purports to be a leading consumer genetics and research company, founded in 2006, that describes its mission as helping people access, understand, and benefit from the human genome. According to the "Corporate Profile" on its website, 23andMe touts itself as having "pioneered direct access to genetic information" and being "the only company with multiple FDA clearances for genetic health reports."[3]

8. As of March 31, 2023, 23andMe cumulatively possesses and stores the Private Information of over 14.1 million people in its databases.[4] This Private Information includes genetic information provided by individuals since 2006 in connection with the Company's "Personal Genome Service" business, which purports to provide consumers "with a broad suite of genetic reports, including information on customers' genetic ancestral origins, personal genetic health

[3] 23andMe, *Corporate Profile*, 23andMe, Inc.: Investor Relations, https://investors.23andme.com/ (last visited Dec. 21, 2023); *see also* 23andMe, *23andMe Receives FDA Clearance for Direct-to-Consumer Genetic Test on a Hereditary Prostate Cancer Marker*, 23andMe, Inc.: Press Release (Jan. 10, 2022), https://investors.23andme.com/news-releases/news-release-details/23andme-receives-fda-clearance-direct-consumer-genetic-test.

[4] 23andMe Holding Co., Annual Report (Form 10-K) (May 25, 2023) ("FY 2022 10-K") at 69.

risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medication."[5]

IV. PLAINTIFF

9. Plaintiff Camie Picha is a resident of the State of Washington.

10. Plaintiff Picha is a customer of 23andMe, who purchased a 23andMe kit in June 2022.

11. In June or July 2022, Plaintiff Picha provided a sample of her genetic material to 23andMe for testing. Ms. Picha was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Ms. Picha's Private Information was maintained by 23andMe.

12. Plaintiff Picha learned about the Data Breach from an email she received from 23andMe on or about October 11, 2023. The October 11 email did not state that Ms. Picha's Private Information was compromised, but rather provided limited information about the Data Breach, including that "certain profile information—which a customer creates and chooses to share with their genetic relatives in the DNA Relatives feature—was accessed from individual 23andMe.com accounts . . . without the account users' authorization." This email also made laudatory representations about 23andMe's internal security practices, including the following.

> Security and privacy are the highest priorities at 23andMe. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate. Beginning in 2019, we've offered and encouraged users to use multi-factor authentication (MFA), which provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords.

13. Subsequently, on or about October 23, 2023, Ms. Picha received a second email from 23andMe in which the Company notified Ms. Picha that certain of her Private Information

[5] FY 2022 10-k at 92.

was "exposed to the threat actor" in the Data Breach. Similar to the October 11 email, the October 23 email similarly provided limited information about the Data Breach and made positive representations about the Company's internal security practices.

14. Plaintiff Picha immediately attempted to contact 23andMe to obtain more details about the data breach but was unable to contact anyone at 23andMe.

15. Plaintiff Picha spent considerable time and money researching and responding to the Data Breach. Among other things, she attempted to find information about the nature of the Data Breach, attempted to identify what specific information of hers had been stolen in the Data Breach, changed the password to her 23andMe account as well as the passwords to other online accounts, and reviewed her accounts for fraudulent activity.

16. Plaintiff Picha also spent time and money researching and purchasing identity theft protection services, as 23andMe did not offer Plaintiff Picha any credit monitoring or identity theft protection services as a result of the Data Breach.

17. Also as a result of the Data Breach, Plaintiff Picha spent time placing credit freezes with the three major credit reporting bureaus.

18. In these regards, the Private Information that was accessed in the Data Breach was the kind of highly sensitive information that can be used to commit fraud and identity theft, and it is reasonable and foreseeable that Ms. Picha would take, and will continue to take, necessary measures to protect herself from identity theft and fraud resulting from the disclosure of her Private Information.

19. Through the identity theft protection service she purchased, Plaintiff Picha learned that her personal information has been compromised and is being offered for sale on the dark web.

20. After the Data Breach, Plaintiff Picha experienced a significant increase in unsolicited telephone calls, texts, and emails, including apparent attempts at identity theft and fraud such as phishing. In this regard, Plaintiff Picha used a relatively new email address for her 23andMe account, which is not associated with many other online accounts and did not receive many spam emails prior to the data breach.

21. Plaintiff Picha places significant value in the security of her Private Information.

Plaintiff Picha entrusted her Private Information to 23andMe with the understanding that 23andMe would keep her Private Information secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Plaintiff Picha is very careful about sharing her sensitive Private Information and would not have entrusted her Private Information to 23andMe had she known of its lax data security policies.

22. Plaintiff Picha is extremely concerned about how the theft of her highly sensitive 23andMe Private Information may impact her, including with respect to the security of her other online accounts, her personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. In this regard, Ms. Picha has suffered emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information. This emotional distress has been compounded by the fact that 23andMe has still not fully informed her of key details about the Data Breach.

23. 23andMe thus betrayed Plaintiff Picha's trust and failed to properly maintain the privacy of her Private Information and prevent unauthorized access to that Private Information.

24. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Picha has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach, including but not limited to: (i) lost or diminished value of her Private Information; (ii) lost opportunity costs associated with attempting to mitigate the consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; and (v) the substantial and imminent risk of future harm resulting from the disclosure of her Private Information in the Data Breach.

25. As a result of the Data Breach, Plaintiff Picha is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Picha therefore anticipates spending considerable time and money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

26. Plaintiff Picha has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

27. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed, compromised, and/or stolen during the Data Breach.

28. Accordingly, Plaintiff brings this action, on behalf of herself and all others similarly situated, against 23andMe seeking redress for its unlawful conduct asserting claims on behalf of a nationwide class for (1) negligence, (2) negligence per se, (3) breach of implied contract, (4) unjust enrichment, and (5) declaratory judgment; and on behalf of a Washington statewide subclass for (6) violation of the Washington Data Breach Notice Act, and (7) violation of the Washington Consumer Protection Act.

V. STATEMENT OF FACTS

A. 23andMe Collects, Stores, and Profits from Private Information, and Promises To Keep It Secure.

29. 23andMe purports to be a leading consumer genetics and research company, founded in 2006, that describes its mission as helping people access, understand, and benefit from the human genome. According to the "Corporate Profile" on its website, 23andMe "want[s] to disrupt the healthcare experience by building a personalized health and wellness experience that caters uniquely to the individual by harnessing the power of their DNA" and touts itself as having "pioneered direct access to genetic information" as "the only company with multiple FDA clearances for genetic health reports."[6]

30. As stated in its last annual report filed with the U.S. Securities and Exchange Commission, as of March 31, 2023, 23andMe has approximately 14.1 million customers who have supplied their Private Information to the Company.[7]

31. This Private Information includes PHI, which is considered "the most confidential

[6] 23andMe Investor Relations, *supra* note 3.
[7] FY 2022 10-K at 69, *supra* note 4.

and valuable type of [PII] . . . irrevocable once breached."[8] In this regard, an individual's unique and immutable genetic information is the most confidential and valuable form of PHI.

32. Similarly, this Private Information includes genetic information provided by individuals since 2006 in connection with the Company's "Personal Genome Service" business, which purports to provide consumers "with a broad suite of genetic reports, including information on customers' genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medication."[9]

33. In order for 23andMe to offer its services to customers including Plaintiff and the Class Members, Plaintiff and Class Members were required to transfer possession of their Private Information—including their personal genetic material—to 23andMe. 23andMe thereby acquires and electronically stores Private Information provided to it by its customers, and 23andMe was therefore required to ensure that Plaintiff's and Class Members' Private Information was not disclosed or disseminated to unauthorized third parties.

34. Through the possession and use of Plaintiff's and Class Members' Private Information—including an individual's unique genetic information, which is the most sensitive information possible—23andMe assumed duties owed to Plaintiff and Class Members to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures. Therefore, 23andMe knew or

---

[8] Junyuan Ke, et al., *My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach*, SSRN, 7 (Feb. 10, 2022), https://ssrn.com/abstract=4029103. (Under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 1320d, et seq., PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. *See also* 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered PHI under HIPAA, as are genetic data, national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information.) *See also Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health & Human Servs. (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[9] FY 2022 10-K at 92, *supra* note 4.

should have known that it was responsible for safeguarding Plaintiff's and Class Members' Private Information from unauthorized access and misuse.

35. 23andMe has publicly touted its data security and cybersecurity abilities, including stating that the Company "is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected" and that it "take[s] security seriously."[10]

36. 23andMe assures customers that "[y]our privacy comes first."[11] "When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."[12]

37. 23andMe's customers are also told that their genetic data will not be shared with third parties "without your explicit consent" and that "[y]our data is fiercely protected by security practices that are regularly reviewed an updated" and the Company is "doing everything in our power to keep your personal data safe."[13]

38. 23andMe was aware of methods that would provide additional, heightened security that would safeguard its customers' highly sensitive data from unauthorized access and disclosure, including but not limited to requiring users to change their passwords frequently, requiring the use of "strong" passwords, and mandating the use of multi-factor authentication ("MFA") that would require its customers to enter more information than just a single password to access their accounts. Indeed, 23andMe acknowledges that, while MFA "provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords," it only "offered and encouraged" use of MFA starting in 2019.[14]

39. 23andMe claims that it "is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected" and that it "take[s]

[10] 23andMe Blog, *supra* note 2.
[11] 23andMe, *Your privacy comes first*, 23andMe Inc.: Privacy, https://www.23andme.com/privacy/ (last visited Dec. 21, 2023).
[12] *Id.*
[13] *Id.*
[14] 23andMe Blog, *supra* note 2.

security seriously."[15] Moreover, the Company claims that:

> [W]e exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate.[16]

40. Likewise, 23andMe promises that "Privacy is in our DNA," and Jacquie Haggarty, 23andMe's Vice President, General Counsel, and Privacy Officer, represents that "We believe it's our responsibility to provide a safe place for people to explore their DNA," on account of which 23andMe's "commitment to privacy is built on a foundation of transparency and choice—our customers know that they are always in control of their data."[17]

41. 23andMe similarly recognizes that "[w]hen you explore your DNA with 23andMe, you entrust us with important personal information," and "since day one, protecting your privacy has been our number one priority."[18] 23andMe further reassures its customers that "[y]ou are in control of your data," and "you decide how your information is used and with whom it is shared."[19]

42. Plaintiff and Class Members entrusted their Private Information to 23andMe, its officials, and agents. Plaintiff and Class Members relied on 23andMe to keep their Private Information secure and safeguarded against unauthorized access and disclosure to unauthorized persons. 23andMe owed a duty to Plaintiff and Class Members to secure their Private Information and ultimately breached that duty, as Plaintiff's and Class Members' Private Information was compromised, unlawfully accessed, and exfiltrated due to the Data Breach.

B. Despite Its Promises, 23andMe Failed To Protect Plaintiff's Private Information.

43. Despite its promises, 23andMe and its employees failed to properly monitor the

---

[15] *Id.*
[16] *Id.*
[17] 23andMe, *What you should know about privacy at 23andMe*, 23andMe, Inc.: Privacy overview, https://www.23andme.com/legal/privacy/ (last visited Dec. 21, 2023).
[18] *Your privacy comes first*, 23andMe Inc.: Privacy, *supra* note 11.
[19] *Id.*

computer network and systems in which the Private Information of Plaintiff and Class Members was maintained, and 23andMe failed to detect and stop the Data Breach. Had 23andMe properly monitored its systems and employed appropriate security measures commensurate with the sensitivity of the Private Information, it would have either discovered the intrusion sooner or been able to prevent it entirely.

44. According to news reports, on or about August 11, 2023, "a hacker on a known cybercrime forum called Hydra advertised a set of 23andMe user data."[20] The hacker claimed "to have 300 terabytes of stolen 23andMe user data" that it would sell for $50 million, and offered to sell "a subset of data" for between $1,000 and $10,000.[21] The hacker also purportedly indicated that they had contacted 23andMe, "'but instead of taking the matter seriously, [the Company] asked irrelevant questions.'"[22] At least one person saw the hacker's August 11, 2023 post in the Hydra forum and sought to alert 23andMe users on an unofficial 23andMe user forum on Reddit that same day.[23]

45. For nearly two months, 23andMe did nothing in response to the August 11, 2023 Hydra and Reddit posts, leaving Plaintiff and Class Members uninformed about the Data Breach, while their Private Information was for sale to criminals on the dark web, and unauthorized parties accessed and viewed Plaintiff's and Class Members' unencrypted, unredacted Private Information, including their highly sensitive genetic data.

46. In early October 2023, 23andMe user data misappropriated in the Data Breach appeared for sale on another hacking forum called BreachForums, including data that was claimed to come from "one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users."[24] Subsequently, "the actor began selling what it claims are 23andMe profiles for

---

[20] Lorenzo Franceschi-Bicchierai et al., *Hackers advertised 23andMe stolen data two months ago*, TechCrunch (Oct. 10. 2023), https://techcrunch.com/2023/10/10/hackers-advertised-23andme-stolen-data-two-months-ago/.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

between $1 and $10 per account, depending on the scale of the purchase."[25]

47. Defendant did not acknowledge or address the Data Breach until October 6, 2023, when it announced, via a blog post on its website (the "October 6 Blog Post"), that the Company had "recently learned that certain 23andMe customer profile information . . . was compiled from individual 23andMe.com accounts without the account users' authorization" as a result of "threat actors" being able to "access certain accounts."[26] The October 6 Blog Post attempted to shift responsibility to 23andMe users, expressing Defendant's "belie[f]" that the Data Breach was the result of "threat actors [who] were able to access certain accounts in instances where users recycled login credentials—that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked."[27]

48. 23andMe's October 6 Blog Post did not provide any details on how many people were affected by the Data Breach and failed to mention that hackers had been selling 23andMe user data on the dark web for nearly two months because of the Data Breach.

49. While the October 6 Blog Post did not expressly indicate the scope of the Data Breach in terms of the numbers of users affected or recite the categories of Private Information that were exposed, compromised, and stolen by unauthorized third parties, the categories of information in the "DNA Relatives feature" referenced by Defendant include:

i. Names;

ii. Sex;

iii. Dates of Birth;

iv. Genetic Information that includes (but is not limited to);

a. Maternal and Paternal Haplogroup results;

b. Neanderthal Ancestry results;

v. Predicted relationships with genetic matches;

---

[25] Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023, 5:53 PM), https://www.wired.com/story/23andme-credential-stuffing-data-stolen/.

[26] 23andMe Blog, *supra* note 2.

[27] *Id.*

vi. Ancestry reports;

vii. Ancestors' birth locations and family names;

viii. Family tree information;

ix. Profile pictures; and

x. Geographic location.[28]

50. The October 6 Blog Post, and subsequent updates thereto also do not include information about the cause of the Data Breach, the vulnerabilities exploited, and any remedial measures taken to ensure that such a breach does not occur again.

51. 23andMe updated its October 6 Blog Post on October 9, 2023 to report, among other things, that it had recently engaged a third-party forensic expert and was "working with federal law enforcement."[29] Then, on October 20, 2023, 23andMe announced that it had temporarily disabled certain features on the DNA relatives tool. The October 6 Blog Post and the two subsequent updates thereto failed to provide basic details concerning the Data Breach, including whether the breach was a system-wide breach, how many people were affected by the Data Breach, and whether certain populations, ethnic groups, or other identifiable categories of individuals were targeted in the cyberattack.

52. On November 6, 2023, 23andMe updated its October 6 Blog Post to report that "[s]tarting today, we are requiring all customers to utilize 2-step verification (2SV) as an added layer of protection for their account.[30]

53. On December 1, 2023, 23andMe again updated its October 6 Blog Post to report that "23andMe has completed its investigation, assisted by third-party forensic experts," and is "in the process of notifying affected customers, as required by law."[31]

54. Finally, on December 5, 2023, 23andMe again updated its October 6 Blog Post, stating that "[a]s our investigation comes to a close, we wanted to share the details of what took

[28] 23andMe Customer Care, *DNA Relatives Privacy & Display Settings*, 23andMe, Inc., https://customercare.23andme.com/hc/en-us/articles/212170838 (last visited Dec. 21, 2023).
[29] 23andMe Blog, *supra* note 2.
[30] *Id.*
[31] *Id.*

place and our findings," including the following information.

> The threat actor used the compromised accounts to access information shared with these accounts. Specifically, DNA Relatives profiles connected to these compromised accounts, which consist of information that a customer chooses to make available to their genetic relatives when they opt in to participate in 23andMe's DNA Relatives feature. A DNA Relatives profile includes information such as display name, predicted relationships, and percentage of DNA shared with matches. . . .
>
> Additionally, through the compromised accounts, the threat actor accessed a feature called Family Tree, which includes a limited subset of DNA Relatives profile information. The Family Tree feature does not include ancestry information such as the percentage of DNA shared with genetic matches or ancestry reports.
>
> Additional Details
>
> - The threat actor was able to access less than 0.1%, or roughly 14,000 user accounts, of the existing 14 million 23andMe customers through credential stuffing.
>
> - The threat actor used the compromised credential stuffed accounts to access the information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million), each of which were connected to the compromised accounts.[32]

C. 23andMe Compounded Its Failure By Providing Inadequate Notice.

55. 23andMe's notice to Plaintiff and Class Members was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including but not limited to how unauthorized third parties were able to access Private Information, what Private Information was in fact compromised, and how many people were affected by the Data Breach.

56. It is well-documented that:

> [t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[33]

---

[32] *Id.*

[33] Javelin Strategy & Research, *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire

57. Here, the same applies to 23andMe and the unauthorized access to Plaintiff's and Class Members' accounts.

58. Indeed, once a data breach has occurred,

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers . . . If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves.[34]

59. Although their Private Information was improperly exposed on or before August 11, 2023, Plaintiff and Class Members were not notified until October 6, 2023. 23andMe's delay deprived Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

60. As a result of 23andMe's delay in detecting and notifying individuals of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher, a warning state Attorneys General have alluded to when questioning 23andMe about its "unreasonable delay" in notifying affected consumers about the Data Breach.[35]

61. 23andMe's efforts to notify Plaintiff and Class Members thus fell short of providing key information about the Data Breach, consisting of brief messages with little substantive information that failed to sufficiently warn victims to take action to protect themselves from identity theft and fraud.

62. 23andMe's deficient notices compounded the harm suffered by Plaintiff and Class Members, by failing to timely provide Breach victims with the very details necessary to protect themselves.

(Feb. 1, 2017), https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[34] Allen St. John, *The Data Breach Next Door*, Consumer Reports (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

[35] William Tong, Att'y Gen. of Connecticut, Letter to Jacquie Cooke, General Counsel and Privacy Officer for 23andMe re: Data Breach (Oct. 30, 2023), https://portal.ct.gov/-/media/AG/Press_Releases/2023/10-30-2023-William-Tong--23andMe-Inc-Inquiry-Letter-final-002.pdf.

D. 23andMe Failed To Comply With Regulatory Guidance and Industry-Standard Cybersecurity Practices.

63. 23andMe's Data Breach is attributable to its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII and PHI.

64. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access. California is one such state and requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

65. 23andMe also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

66. The FTC recommends, among other things:

- limiting access to customer information to those who have a legitimate business need for it;
- encrypting customer information on system and in transit;
- implementing multi-factor authentication for anyone accessing customer information;
- implementing procedures and controls to monitor when authorized users are accessing customer information;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information; and

- implementing procedures and controls to detect unauthorized access to customer information, including monitoring activity logs for signs of unauthorized access to customer information.[36]

67. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[37]

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[38] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

69. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

70. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates

---

[36] *See* Federal Trade Commission, *FTC Safeguards Rule: What Your Business Needs to Know*, available at https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

[37] Federal Trade Commission, *Start With Security: A Guide for Business*, at 2 (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[38] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

73. 23andMe was aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers' PII from unauthorized access. In this case, 23andMe was at all times fully aware of its obligation to protect the PII of its customers. 23andMe was also aware of the significant repercussions if it failed to do so because 23andMe collected PII from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiff and Class Members.

74. Based upon the known details of the Data Breach and how it occurred, 23andMe also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to rate limiting, user-activity monitoring, and data-loss prevention.

75. Defendant is also a covered Business Associate under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information") , 45 C.F.R. Part 160 and Part 164, Subparts A and C.

76. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[39] See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[39] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

77. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

78. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

79. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

80. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

81. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

82. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

83. HIPAA and HITECH also obligated 23andMe to implement policies and

procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. See 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

84. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires 23andMe to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following the discovery of a breach."[40]

85. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

86. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

87. HIPAA also requires the Office of Civil Rights ("OCR") within the Department of Health and Human Services ("HHS") to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[41] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard

[40] Breach Notification Rule, U.S. Dep't of Health & Human Servs. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

[41] Security Rule Guidance Material, U.S. Dep't of Heath & Human Servs. (Oct. 18, 2023), http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

for good business practices with respect to standards for securing e-PHI."[42]

E. The Effect of the Data Breach on Plaintiff and Class Members.

88. 23andMe's failure to keep Plaintiff's and Class Members' Private Information secure has severe ramifications. Given the sensitive nature of the Private Information stolen in the Data Breach—including name, sex, date of birth, genetic information, predicted relationships with genetic matches, ancestry reports, ancestors' birth locations and family names, family tree information, profile pictures, and geographic location—cybercriminals can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury, including actual or attempted identity theft, fraud, or related cybercrimes due to the Data Breach.

89. Armed with the Private Information accessed in the Data Breach, data thieves can use that data to commit a variety of crimes, including using Class Members' genetic, health, and ethnic information to target other phishing and hacking intrusions based upon their individual health needs or ethnic backgrounds. Moreover, data thieves or malicious actors who may have purchased or otherwise obtained Private Information from those who stole it may use that data to target Plaintiff and Class Members with violence or threats of harm based on animus toward members of particular ethnic groups. Indeed, the fact that initial leaks of Private Information stolen in the Data Breach and "advertised [for sale] on BreachForums allegedly contain one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users"[43] has prompted at least one State Attorney General to observe that "the increased frequency of antisemitic and anti-Asian rhetoric and violence in recent years means that this may be a particularly dangerous time for such targeted information to be released to the public."[44]

90. Further, malicious actors often wait months or years to use the PII and/or PHI

[42] Guidance on Risk Analysis, U.S. Dep't of Health & Human Servs. (July 22, 2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

[43] Lorenzo Franceschi-Bicchierai et al., *Hackers advertised 23andMe stolen data two months ago,* supra note 20.

[44] William Tong Letter (Oct. 30, 2023), *supra* note 31.

obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII and/or PHI, meaning individuals can be the victim of several instances of identity theft, fraud, or other cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the PII and/or PHI and identifies the victims as 23andMe's customers materially increases the risk to Plaintiff and the Class.

91. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[45] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor her accounts for years to ensure her PII obtained in the Data Breach is not used to harm her. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach. In other words, Plaintiff has been harmed by the value of identity protection services she must purchase in the future to ameliorate the risk of harm she now faces due to the Data Breach.

92. As such, these harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information, as data thieves and malicious actors who purchase the stolen Private Information will continue to use the information to the detriment of Plaintiff and Class Members for many years to come.

93. As a direct result of the Data Breach, Plaintiff and Class Members have suffered actual and attempted identity theft and fraud, and they will continue to be exposed to a heightened and imminent risk of identity theft and fraud, potentially for the rest of their lives. Plaintiff and

[45] U.S. Gov't Accountability Off., *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

Class Members must now and in the future closely monitor their medical, insurance, and financial accounts to guard against identity theft and fraud.

94. For this reason, Class Members may incur out-of-pocket costs for purchasing protective measures to deter and detect identity theft and fraud, as well as protective measures to mitigate against the misuse of their genetic information and related Private Information.

95. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiff and Class Members have suffered, and will continue to suffer, damages and economic losses in the form of lost time needed to take appropriate measures to avoid the misuse of their Private Information, potential unauthorized and fraudulent charges, and dealing with spam phone calls, letters, text messages, and emails received as a result of the Data Breach and the unauthorized disclosure and misuse of their Private Information.

96. Plaintiff and Class Members have also realized harm in the lost or reduced value of their Private Information. Plaintiff's Private Information is not only valuable to 23andMe, but Plaintiff also places high value on her Private Information based on her understanding that her Private Information is a financial asset to companies that collect it.[46]

97. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiff's Private Information that was permitted without authorization by 23andMe. This market value for access to PII and/or PHI can be determined by reference to both legitimate and illegitimate markets for such information.

98. Moreover, Plaintiff and Class Members value the privacy of this information and expect 23andMe to allocate enough resources to ensure it is adequately protected. Plaintiff and other customers would not have done business with 23andMe, provided their Private Information, or paid the same prices for 23andMe's goods and services had they known 23andMe did not implement reasonable security measures to protect their Private Information. Customers

[46] *See, e.g.*, Ponemon Institute, LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers*, at 14 (Mar. 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70), https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

reasonably expect that the payments they made to 23andMe incorporate the costs to implement reasonable security measures to protect their Private Information. As a result, Plaintiff and Class Members did not receive the benefit of their bargain with 23andMe because they paid a value for services they expected but did not receive.

99. Given 23andMe's failure to protect Plaintiff's and the Class Members' Private Information, Plaintiff has a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects her from suffering further harm, as her Private Information remains in 23andMe's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on a large class of persons.

100. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their Private Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Private Information; (iii) loss of value of their Private Information; (iv) the lost value of access to Plaintiff's and Class Members' Private Information permitted by 23andMe; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; (vi) 23andMe's retention of profits attributable to Plaintiff's and Class Members' Private Information that 23andMe failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to 23andMe for services purchased, as Plaintiff reasonably believed a portion of the sale price would fund reasonable security measures that would protect her PII, which was not the case; and (x) nominal damages.

VI. CLASS ACTION ALLEGATIONS

A. NATIONWIDE CLASS

101. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

All natural persons residing in the United States whose Private Information was exfiltrated in the Data Breach.

102. The Nationwide Class asserts claims against 23andMe for negligence (Count 1), negligence per se (Count 2), breach of implied contract (Count 3), unjust enrichment (Count 4), and declaratory judgment (Count 5).

B. WASHINGTON SUBCLASS

103. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of a Washington Subclass in the alternative to the nationwide claims (Counts 1 through 5), as well as with respect to statutory claims under the Washington Data Breach Notice Act, Wash. Rev. Code §§ 19.255.010, *et seq.* (Count 6), and the Washington Consumer Protection Act, Wash. Rev. Code. Ann. §§ 19.86.020, *et seq.* (Count 7), on behalf of a Washington Subclass, defined as follows:

All natural persons residing in Washington whose Private Information was exfiltrated in the Data Breach.

104. Excluded from the Nationwide Class and the Washington Subclass (collectively, the "Class") are 23andMe, any entity in which 23andMe has a controlling interest, and 23andMe's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

105. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Nationwide Class and the Washington Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, 23andMe has acknowledged that millions of individuals' PII has been compromised. Those individuals' names and addresses are available from 23andMe's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of individuals in the Nationwide Class and at least thousands of individuals in the Washington Statewide Subclass, making joinder of all Class Members impracticable.

106. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to both the Nationwide Class and the Washington Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include:

1. Whether 23andMe had a duty to protect Private Information;
2. Whether 23andMe failed to take reasonable and prudent security measures to ensure the Private Information it maintains was protected;
3. Whether 23andMe failed to take available steps to prevent and stop the Data Breach from happening;
4. Whether 23andMe knew or should have known that the Private Information it maintains was vulnerable to compromise;
5. Whether 23andMe was negligent in failing to implement reasonable and adequate security procedures and practices;
6. Whether 23andMe's security measures to protect the Private Information it maintains were reasonable in light known legal requirements;
7. Whether 23andMe's conduct constituted unfair or deceptive trade practices;
8. Whether 23andMe violated state or federal law when it failed to implement reasonable security procedures and practices;
9. Which security procedures and notification procedures 23andMe should be required to implement;
10. Whether 23andMe has a contractual obligation to provide for the security of customer Private Information;
11. Whether 23andMe has complied with any contractual obligations to protect customer Private Information;
12. What security measures, if any, must be implemented by 23andMe to comply with its contractual obligations;
13. Whether 23andMe violated state consumer protection laws in connection with the actions described herein;
14. Whether 23andMe failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Data Breach was discovered;
15. Whether 23andMe's conduct resulted in or was the proximate cause of the loss of the Private Information of Plaintiff and Class Members;
16. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of 23andMe's failure to reasonably protect their Private Information;

17. Whether 23andMe should retain the money paid by Plaintiff and Class Members to protect their Private Information, and the profits 23andMe generated through Plaintiff's and Class Members' Private Information;

18. Whether and how 23andMe should retain Plaintiff's and Class Members' valuable Private Information; and,

19. Whether Plaintiff and Class Members are entitled to damages or injunctive relief.

107. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Nationwide Class and the Washington Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's Private Information was in 23andMe's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members, and Plaintiff seeks relief consistent with the relief of the Class.

108. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Nationwide Class and the Washington Subclass because Plaintiff is a member of the Nationwide Class and the Washington Subclass and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

109. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs

may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against 23andMe, and thus, individual litigation to redress 23andMe's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

110. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for 23andMe or would be dispositive of the interests of members of the proposed Class.

111. **Ascertainability.** The Nationwide Class and Washington Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Nationwide Class and Washington Subclass consist of individuals who provided their Private Information to 23andMe. Class Membership can be determined using 23andMe's records.

112. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). 23andMe, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

113. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

VII. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT ONE — NEGLIGENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

114. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

115. 23andMe required Plaintiff and Class Members to submit sensitive Private Information in order to obtain its services.

116. 23andMe owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Private Information in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing 23andMe's security systems to ensure that Plaintiff's and Class Members' Private Information in 23andMe's possession was adequately secured and protected; (b) implementing processes that would detect unauthorized access to the Private Information it maintains in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding unauthorized access to the Private Information it maintains; and (d) maintaining data security measures consistent with industry standards.

117. 23andMe's duty to use reasonable care arose from several sources, including but not limited to those described herein.

118. 23andMe had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by 23andMe's failure to protect their Private Information because hackers routinely attempt to steal such information and use it for nefarious purposes, 23andMe knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

119. 23andMe's duty to use reasonable security measures also arose as a result of the

special relationship that existed between 23andMe, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted 23andMe with their highly sensitive Private Information as part of the purchase of the services 23andMe offers. 23andMe alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

120. 23andMe's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Private Information by companies such as 23andMe. Various FTC publications and data security breach orders further form the basis of 23andMe's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

121. 23andMe's duty also arose from 23andMe's superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the 23andMe Data Breach.

122. 23andMe admits that it has a responsibility to protect the Private Information with which it is entrusted.

123. 23andMe knew or should have known that its data storage architecture were vulnerable to unauthorized access and targeting by cybercriminals for the purpose of stealing and misusing confidential Private Information.

124. 23andMe also had a duty to safeguard the Private Information of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require 23andMe to reasonably safeguard sensitive Private Information, as detailed herein.

125. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid or mitigate identity theft or fraud, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by 23andMe's misconduct.

126. 23andMe breached the duties it owed to Plaintiff and Class Members described

above and thus was negligent. 23andMe breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Private Information of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Private Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' Private Information in 23andMe's possession had been or was reasonably believed to have been, stolen or compromised.

127. But for 23andMe's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

128. 23andMe's failure to take proper security measures to protect the sensitive Private Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' Private Information.

129. Plaintiff and Class Members were foreseeable victims of 23andMe's inadequate data security practices, and it was also foreseeable that 23andMe's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

130. As a direct and proximate result of 23andMe's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit

scores and ratings; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT TWO — NEGLIGENCE *PER SE*

On Behalf of Plaintiff and the Nationwide Class,
or Alternatively, on Behalf of Plaintiff and the Washington Subclass

131. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

132. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as 23andMe of failing to use reasonable measures to protect Private Information.

133. The FTC publications and orders also form the basis of 23andMe's duty.

134. 23andMe violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. 23andMe's conduct was particularly unreasonable given the nature and amount of Private Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving the highly sensitive Private Information it maintains, including specifically the damages that would result to Plaintiff and Class Members.

135. In addition, under state data security statutes, 23andMe had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

136. 23andMe's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

137. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

138. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

139. 23andMe breached its duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiff's and Class Members' Private Information.

140. Plaintiff and Class Members were foreseeable victims of 23andMe's violations of the FTC Act and state data security statutes. 23andMe knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and Class Members.

141. But for 23andMe's violation of the applicable laws and regulations, Plaintiff's and Class Members' Private Information would not have been accessed by unauthorized parties.

142. As a direct and proximate result of 23andMe's negligence per se, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT THREE — BREACH OF IMPLIED CONTRACT

**On Behalf of Plaintiff and the Nationwide Class,
or Alternatively, on Behalf of Plaintiff and the Washington Subclass**

143. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

144. Plaintiff and Class Members entered into an implied contract with 23andMe when they obtained services from 23andMe, or otherwise provided Private Information to 23andMe.

145. As part of these transactions, 23andMe agreed to safeguard and protect the Private Information of Plaintiff and Class Members and to timely and accurately notify them if their Private Information was breached or compromised.

146. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that 23andMe's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiff and Class Members believed that 23andMe would use part of the monies paid to 23andMe under the implied contracts or the monies obtained from the benefits derived from the Private Information they provided to fund adequate and reasonable data security practices.

147. Plaintiff and Class Members would not have provided and entrusted their Private Information to 23andMe or would have paid less for 23andMe products or services in the absence of the implied contract or implied terms between them and 23andMe. The safeguarding of the Private Information of Plaintiff and Class Members was critical to realize the intent of the parties.

148. Plaintiff and Class Members fully performed their obligations under the implied contracts with 23andMe.

149. 23andMe breached its implied contracts with Plaintiff and Class Members to protect their Private Information when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

150. As a direct and proximate result of 23andMe's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at

trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT FOUR — UNJUST ENRICHMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

151. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

152. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by 23andMe and that was ultimately stolen in the 23andMe Data Breach.

153. 23andMe was benefitted by the conferral upon it of the Private Information pertaining to Plaintiff and Class Members and by its ability to retain, use, and profit from that information. 23andMe understood that it was in fact so benefitted.

154. 23andMe also understood and appreciated that the Private Information pertaining to Plaintiff and Class Members was private and confidential and its value depended upon 23andMe maintaining the privacy and confidentiality of that Private Information.

155. But for 23andMe's willingness and commitment to maintain its privacy and

confidentiality, that Private Information would not have been transferred to and entrusted with 23andMe.

156. Because of its use of Plaintiff's and Class Members' Private Information, 23andMe sold more services than it otherwise would have. 23andMe was unjustly enriched by profiting from the additional services it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

157. 23andMe also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' Private Information.

158. 23andMe also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiff's and Class Members' Private Information.

159. It is inequitable for 23andMe to retain these benefits.

160. As a result of 23andMe's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the unauthorized disclosure of that Private Information), 23andMe has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

161. 23andMe's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from unauthorized access by hackers and identity thieves.

162. It is inequitable, unfair, and unjust for 23andMe to retain these wrongfully obtained benefits. 23andMe's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

163. The benefit conferred upon, received, and enjoyed by 23andMe was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for 23andMe to retain the benefit.

164. 23andMe's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused the Plaintiff and Class Members other damages as described herein.

165. Plaintiff and the Class Members have no adequate remedy at law.

166. 23andMe is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on 23andMe as a result of its wrongful conduct, including specifically: the value to 23andMe of the Private Information that was stolen in the Data Breach; the profits 23andMe received and is receiving from the use of that information; the amounts that 23andMe overcharged Plaintiff and Class Members for use of 23andMe's products and services; and the amounts that 23andMe should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' Private Information.

COUNT FIVE — DECLARATORY JUDGMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

167. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

168. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

169. An actual controversy has arisen in the wake of the 23andMe Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether 23andMe is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff continues to suffer injury as a result of the compromise of Plaintiff's Private Information and remain at imminent risk that further compromises of her Private Information will occur in the future given the publicity around the Data Breach and the nature and

quantity of the Private Information stored by 23andMe.

170. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. 23andMe continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. 23andMe continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

171. The Court also should issue corresponding prospective injunctive relief requiring 23andMe to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

172. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at 23andMe. The risk of another such breach is real, immediate, and substantial. If another breach at 23andMe occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

173. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to 23andMe if an injunction is issued. Among other things, if another significant data breach occurs at 23andMe, Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to 23andMe of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and 23andMe has a pre-existing legal obligation to employ such measures.

174. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at 23andMe, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

VIII. CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT SIX — VIOLATION OF THE WASHINGTON DATA BREACH NOTICE ACT, WASH. REV. CODE §§ 19.255.010, ET SEQ.

On Behalf of Plaintiff and the Washington Subclass

175. Plaintiff Picha ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

176. 23andMe is a business that owns or licenses computerized data that includes "personal information" as defined by Wash. Rev. Code § 19.255.010(1).

177. Plaintiff's and Class Members' Private Information includes "personal information" as covered under Wash. Rev. Code § 19.255.010(5).

178. 23andMe is required to accurately notify Plaintiff and Class Members following discovery or notification of the breach of its data security program if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

179. Because 23andMe discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, 23andMe had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

180. By failing to disclose the Data Breach to Plaintiff and all Class Members in a timely and accurate manner, 23andMe violated Wash. Rev. Code § 19.255.010(1).

181. As a direct and proximate result of 23andMe's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Class Members suffered damages, as described above.

182. Plaintiff and Class Members seek relief under Wash. Rev. Code §§ 19.255.040, including actual damages and injunctive relief.

COUNT SEVEN — VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, WASH. REV. CODE ANN. §§ 19.86.020, ET SEQ.

On Behalf of Plaintiff and the Washington Subclass

183. Plaintiff Picha ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

184. 23andMe is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

185. 23andMe advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

186. 23andMe engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties

pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

187. 23andMe's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of 23andMe's data security and ability to protect the confidentiality of consumers' Private Information.

188. 23andMe's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Class Members, that their Private Information was not exposed and misled Plaintiff and the Class Members into believing they did not need to take actions to secure their identities.

189. 23andMe acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff's and Class Members' rights.

190. 23andMe's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, et seq. Alternatively, 23andMe's conduct is injurious to the public interest because it has injured Plaintiff and Class Members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Washingtonians affected by the Data Breach.

191. As a direct and proximate result of 23andMe's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Class Members have suffered and will continue

to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

192. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

IX. REQUEST FOR RELIEF

Plaintiff, individually and on behalf of members of the Nationwide Class and Washington Subclass, as applicable, respectfully requests that the Court enter judgment in Plaintiff's favor and against 23andMe, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit 23andMe from continuing to engage in the unlawful acts, omissions, and practices described herein, including;

a. Prohibiting 23andMe from engaging in the wrongful and unlawful acts described herein;

b. Requiring 23andMe to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring 23andMe to delete, destroy and purge the Private Information of Plaintiff and Class Members unless 23andMe can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. Requiring 23andMe to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

e. Requiring 23andMe to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on 23andMe's systems on a periodic basis, and ordering 23andMe to promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring 23andMe to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring 23andMe to audit, test, and train its security personnel regarding any new or modified procedures;

h. Requiring 23andMe to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

i. Requiring 23andMe to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. Requiring 23andMe to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with 23andMe's policies, programs and systems for protecting Private Information;

k. Requiring 23andMe to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor 23andMe's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l. Requiring 23andMe to meaningfully educate all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

m. Requiring 23andMe to implement logging and monitoring programs sufficient to track traffic to and from 23andMe servers; and

n. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis 23andMe's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

3. That the Court award Plaintiff and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by 23andMe as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiff be granted the declaratory relief sought herein;

7. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre-judgment and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

X. DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

RESPECTFULLY SUBMITTED this 29th day of December, 2023.

/s/ Christopher L. Springer
Christopher L. Springer (SBN 291180)
KELLER ROHRBACK L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Tel: (805) 456-1496
cspringer@kellerrohrback.com

Cari Campen Laufenberg (*pro hac vice* forthcoming)
Gretchen Freeman Cappio (*pro hac vice* forthcoming)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 9f8101
Tel: (206) 623-1900
claufenberg@kellerrohrback.com
gcappio@kellerrohrback.com